DOI: 10.3969/j.issn.1674-7135.2024.01.012

量子通信技术及应用研究综述

李冲霄[1,2],李 卓[1]

(1. 西安电子科技大学 通信工程学院,西安 710071; 2. 中国电子科技集团公司第五十四研究所,石家庄 050081)

摘 要: 量子通信技术自 20 世纪 80 年代诞生以来,获得了突飞猛进的发展。文章将量子通信技术及应用研究划分为量子通信协议研究、量子通信工程技术研究以及量子通信应用研究等三方面。在对量子密钥分发、量子秘密共享、量子隐形传态和量子安全直接通信等量子通信协议的技术原理、应用领域和研究进展进行分析对比的基础上,对量子光源产生、量子随机数发生、量子纠缠编码和单光子探测等量子通信工程技术的研究现状进行了总结,并对当前世界各国在量子通信链路构建、量子通信网络构建和量子通信系统构建等方面的主要研究进展进行了介绍,指出了量子通信当前存在的通信速率低、传输距离近、制造成本高等问题,明确了未来的发展方向,可以为量子通信技术和应用相关研究提供一定的参考。

关键词: 量子通信技术; 量子通信应用; 量子纠缠

中图分类号: V443; TN918.1 **文献标志码:** A **文章编号:** 1674-7135(2024)01-0072-09

Overview of quantum communication technology and application research

LI Chongxiao[1,2], LI Zhuo[1]

(1. School of Communication Engineering, Xidian Univetsity, Xi'an 710071, China;
2. The 54th Research Institute of CETC, Shijiazhuang 050081, China)

Abstract: Quantum communication technology has undergone rapid development since its inception in the 1980s. This article divides quantum communication technology and application research into three aspects: quantum communication protocol research, quantum communication engineering technology research, and quantum communication application research. On the basis of analyzing and comparing the technical principles, application fields, and research progress of quantum communication protocols such as quantum key distribution, quantum secret sharing, quantum teleportation, and quantum secure direct communication, this paper summarizes the current research status of quantum communication engineering technologies such as quantum light source generation, quantum random number generation, quantum entanglement coding, and single photon detection. The main research progress in the construction of quantum communication links, quantum communication networks and quantum communication systems in various countries around the world was introduced. The current problems of low communication speed, short transmission distance, and high manufacturing costs in quantum communication was pointed out. The future development direction was clarified, which can provide some references for research related to quantum communication technology and applications.

Key words: quantum communication technology; quantum communication application; quantum entanglement

收稿日期: 2023-10-18; **修回日期:** 2023-12-07

基金项目: 国家自然科学基金(编号: U19B2025)

引用格式: 李冲霄,李卓. 量子通信技术及应用研究综述[J]. 空间电子技术,2024,21(1):72-80. LI C X, LI Z. Overview of quantum communication technology and application research[J]. Space Electronic Technology, 2024, 21(1): 72-80.

0　引言

近年来，量子信息科学研究获得了极大的发展。2021 年，美国 FASER 小组发现了宏观世界铝片膜的量子纠缠现象[1]；2022 年，Alain Aspect 等人因证明贝尔不等式不成立获得诺贝尔物理学奖；2023 年，中科大的潘建伟团队成功进行了 1002 km 的光纤链路无中继量子密钥分发。特别是，我国成功研制出世界最快的光量子计算机 – “九章三号”，能够同时处理 255 个光量子，运算速度比当前世界最快的超级计算机 – “前沿”快 23 个数量级，有力彰显了量子信息科学的神奇魅力[2]。而量子通信就是基于量子力学的海森堡不确定性、波粒二象性和量子纠缠等基本原理，通过对量子态的操作，实现信息安全保密传递的一种通信方式。海森堡不确定性是指微观粒子的位置和动量是一对相互关联的特性，无法同时给出确定的状态，只能给出微观粒子在时空的概率分布。波粒二象性是指微观粒子不同于宏观物体，它既具有波的特性，也具有粒子的特性，两种特性同时存在，相互制约，相互影响。量子纠缠是指相关纠缠的两个微观粒子，无论距离多远，改变其中一个粒子的状态，另一个粒子的状态同时就会发生改变。量子通信是目前人类已知的、唯一可以在数学上证明的、绝对安全的通信方式。自 1984 年，BENNETT C H 和 BRASSARD G 提出了世界上第一个量子通信协议 – BB84 协议以来，人类便拉开了量子通信的研究大幕。后续研究人员又进一步提出了量子隐形传态、量子秘密共享等协议，并尝试将相关理论逐步应用到工程实践，提高通信的安全保密性。

1　量子通信技术及应用研究分类

目前，关于量子通信技术及其应用的研究，主要集中在量子通信协议研究、量子通信工程技术研究以及量子通信应用研究等方面。量子通信协议研究可以为量子通信技术和应用研究提供理论基础；量子通信工程技术研究可以为量子通信应用研究提供实践基础；量子通信应用研究主要基于已有的量子通信协议和量子通信工程技术研究成果，研究和构建实用化量子通信系统。量子通信技术及其应用的研究分类如图 1 所示。

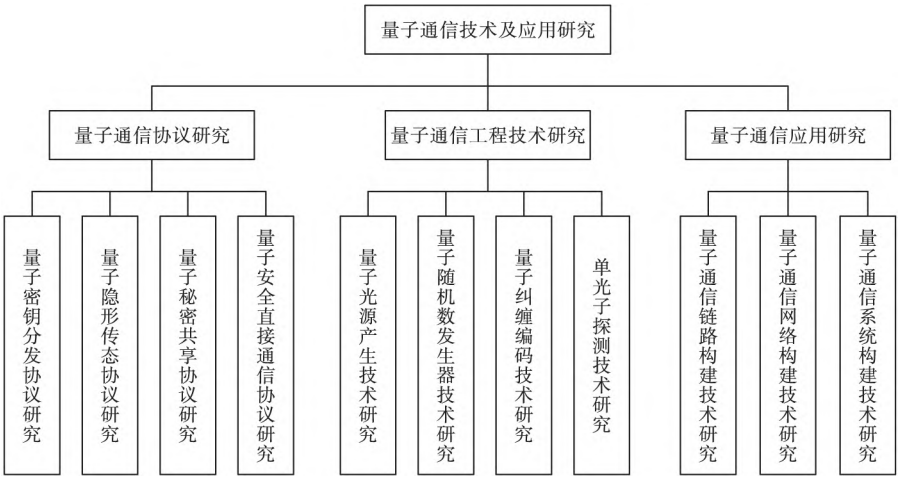

图 1　量子通信技术及其应用研究分类

Fig. 1　Classification of quantum communication technology and its application research

2　量子通信协议研究

量子通信协议研究萌芽于 20 世纪 60 年代[3]，诞生于 20 世纪 80 年代，发展于 20 世纪末至 21 世纪初。量子通信协议研究主要基于量子力学基本原理，设计量子通信协议，为保证信息的安全保密传递提供理论基础。目前，量子通信协议研究基础架构已经基本成型。量子通信协议研究，依据所传输的比特类型以及使用场景，可划分为量子密钥分发、量子秘密共享、量子安全直接通信和量子隐形传态等协议研究。

2.1　量子密钥分发协议

量子密钥分发是基于量子纠缠等量子力学基本原理，进行密钥信息的安全传递。量子密钥分发协议主要分为非纠缠单光子类、纠缠光子类和连续变量类等类型。1984 年，美国物理学家 BENNETT C H 和加拿大密码学家 BRASSARD G，基于量子态的不可克隆和测量坍缩性质，提出了人类历史上第

一个用于量子密钥分发的通信协议—BB84 协议[4]。这一年被称为量子通信元年。BB84 协议属于非纠缠单光子类密钥分发协议。该协议使用量子信道叠加经典信道的方式进行通信，基于量子信道进行光子的偏振态来传输，基于经典信道进行收发双方测量基矢的比对，根据比对结果生成密钥。该协议在分发密钥的同时，可有效检测窃听；为了解决 BB84 协议的复杂性问题，BENNETT C H 于 1992 年提出了简化版的 BB84 协议—B92 协议[5]；1991 年，美国物理学家 EKERT AK 基于量子纠缠提出了 E91 协议[6]，相比 BB84 协议的单光子传输，E91 协议先在本地生成纠缠光子对，然后分别发送给通信双方，使双方基于量子纠缠产生通信密钥；为了解决 BB84 协议和 E91 协议存在的必须使用价格昂贵的光子测量器件的问题，1999 年，拉斐尔等人提出了一种基于光宏观特性的量子密钥分发协议，属于典型的连续变量类协议，降低了量子密钥分发的成本；为了解决密钥分发系统中，由于探测器的安全漏洞而存在的粒子分束攻击等问题，KULIK S P 等人提出了基于诱骗态的 MDI-QKD 协议，该协议与测量设备无关[7]，推动了量子密钥分发技术由理论向应用的发展。量子密钥分发通信原理如图 2 所示。

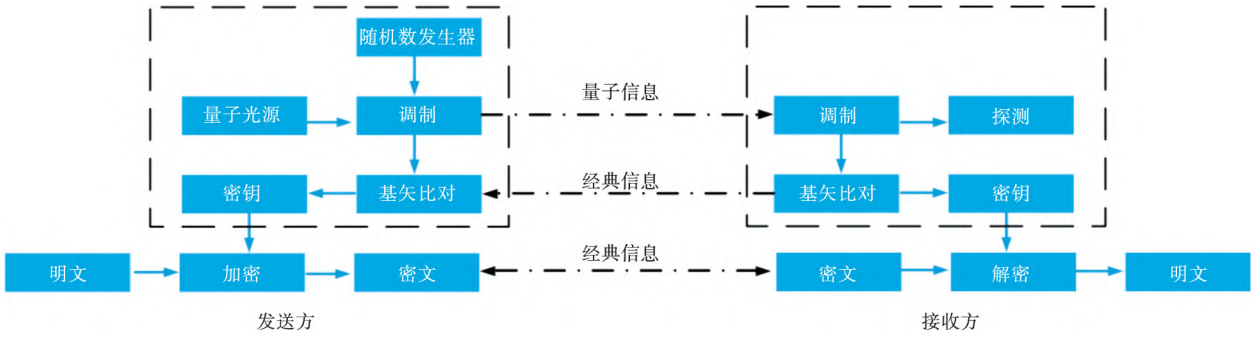

图 2　量子密钥分发通信原理图

Fig. 2　Schematic diagram of quantum key distribution communication

2.2　量子隐形传态协议

量子隐形传态是基于量子纠缠等量子力学基本原理，不发送实际粒子，仅通过发送量子态的概率，就可以将发送方粒子的未知量子态，在接收方粒子上呈现出来。量子隐形传态可以划分为分离变量类、连续变量类和受控变量类等类型。1993 年，BENNETT C H 和 BRASSARD G 等人基于 Bell 态联合测量，提出了人类历史上第一个量子隐形传态方案[8]，属于分离变量类；1998 年，KIMBLE 等人针对分离变量类协议存在探测效率低的问题，提出了一种连续变量类协议，提高了量子态的探测可靠性；2000 年，ZHOU J 等人提出了一种必须在通信双方和第三方都同意时，才能进行量子态隐形传递的协议，提高了通信的可控性；2008 年，JUNG E 等人基于三粒子态和 W 态，提出了单量子比特的隐形传态[9]，进一步丰富和发展了量子隐形传态协议。量子隐形传态通信原理如图 3 所示。

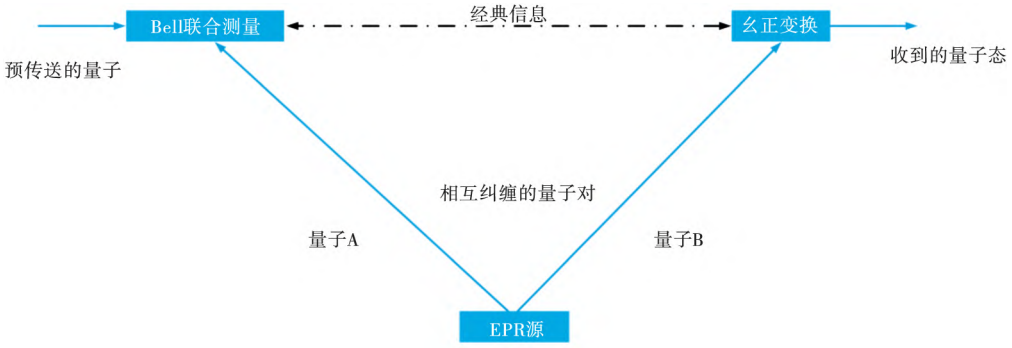

图 3　量子隐形传态通信原理图

Fig. 3　Schematic diagram of quantum teleportation communication

2.3　量子秘密共享协议

量子秘密共享是基于量子纠缠等量子力学基本原理，将秘密信息进行编码、分发和共享。量子秘密共享主要分为单光子类、最大纠缠态类和纠缠

纯态类等类型。1999 年，SHAMIR A 提出了人类历史上第一个量子秘密共享协议—HBB 协议[10]。HBB 协议允许通信多方安全地共享秘密信息并相互制约；2009 年，GAO G 提出了基于双光子三维 Bell 态量子秘密共享协议[11]，解决了大容量的量子秘密共享问题；LI H C M 在 GAO G 等人的基础上，提出了改进型双光子三维 Bell 态量子秘密共享协议，基于诱骗态，提高了窃听检查效率[12]。

2.4　量子安全直接通信协议

量子安全直接通信是基于量子纠缠等量子力学基本原理，直接通过量子信道安全保密地传递信息。量子安全直接通信适用于既要保证通信安全，又时间紧迫的场景，例如投票、竞标、谈判等任务中。所以量子安全直接通信必须要同时解决在线窃听检测和信息前泄露的问题。量子安全直接通信主要分为单光子类和纠缠光子类。2000 年，龙桂鲁和刘晓曙提出了世界上第一个量子安全直接通信协议—高效量子安全直接通信协议[13]。该协议采用数据分块的办法，可有效防止信息前泄露发生；2003 年，邓富国等人依据量子安全直接通信的原理，给出了其详细判断标准，为后续研究提供了理论依据；2004 年，邓富国和龙桂鲁等人基于单光子量子态，设计了一种支持一次一密的量子安全直接通信协议 – DL04 协议；2008 年，邢莉娟等人提出了量子安全直接通信模型[14]，用模块化的方法将通信过程划分为量子信源编译码、量子信道编译码、量子信道和量子噪声等模块；早期的量子安全直接通信协议都是基于理想环境，为了解决实际信道的噪声影响问题，2011 年，顾斌等人提出了抗噪声的量子安全直接通信协议[15]；2020 年，周渊等人提出了与设备无关的量子安全直接通信协议，消除了量子安全直接通信系统实际设备的安全性漏洞；2022 年，龙桂鲁团队成功实现了量子安全直接通信，将量子安全直接通信由理论变成了现实。量子安全直接通信原理如图 4 所示。

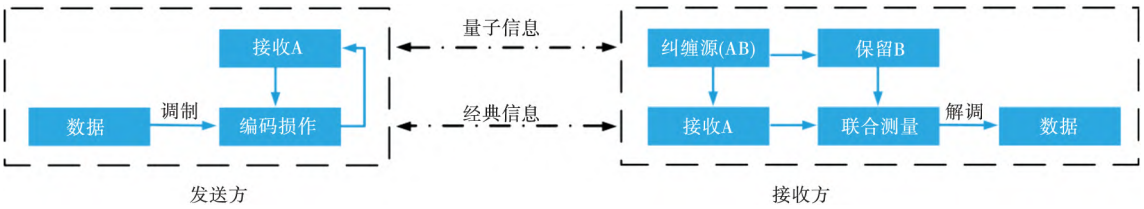

图 4　量子安全直接通信原理图

Fig. 4　Schematic diagram of quantum secure direct communication

关于量子密钥分发、量子秘密共享和量子隐形传态等量子通信协议的研究起步较早，研究成果也较为丰硕。目前，量子通信协议的研究框架已基本成型，能够为量子通信应用提供基本理论支撑。主要量子通信协议如表 1 所列。

表 1　主要量子通信协议

Tab. 1　Main quantum communication protocols

量子通信协议	技术原理	应用领域	典型协议代表
量子密钥分发	利用量子力学不确定性、不可克隆、量子纠缠等原理进行密钥信息分发	适用于点对点密钥信息保密分发	BB84、B92、E91
量子隐形传态	利用量子纠缠等原理进行量子信息的隐蔽传递	适用于用户间的保密通信	连续变量隐形传态
量子秘密共享	利用量子纠缠等原理进行秘密信息的编码和共享	适用于多用户之间的秘密信息安全分享	HBB 协议
量子安全直接通信	利用量子纠缠和块传输等技术，进行用户间点对点安全直接通信	适用于既要保证通信安全，又时间紧迫的场景	一次一密量子安全直接通信

3　量子通信工程技术研究

量子通信工程技术研究主要是解决量子通信技术由理论到应用的工程技术问题。量子通信应用研究主要包括量子光源产生、量子随机数发生、量子纠缠编码和单光子探测等方面。目前，关于量子光源产生、量子随机数发生、量子纠缠编码和单光子探测等方面的研究，已经取得了一定成绩，但是距离量子通信工程技术成熟落地尚有一定距离。

3.1　量子光源产生技术

量子光源产生技术，主要是为量子通信提供传

输载体。包括单光子源和纠缠光源等类型。单光子源一个脉冲里只有一个光子，而纠缠光源则会产生来自同一光束的两个相互纠缠的光子。量子光源产生器是发送端的重要组成部分。1997 年，KIMBLE 等人采用激光共振的方式，对钠原子束进行激发，开启了相干原子产生技术的大门，能够进行 nm 级别的微观操控，有助于高精度测量系统的制造[16]。受其启发，研究人员分别基于单粒子辐射和相干光衰减的方法产生了单光子。通常，单粒子辐射光源体积较为庞大，产生光子效率较低且无法预测。相比而言，相干光衰减光源体积较小且稳定性较高，优势较为明显[17]。1988 年，WANG X L 等人提出了一种由自发参量转化生成光子对的方法，拉开了纠缠光源产生的序幕[18]。2010 年，Ch. Heyn 通过在砷化铝镓(aluminum gauium arsenide，AlGaAs)和砷化铝(Alumioum arsenlid，AlAs)中填充纳米孔制备光子的方法产生了纠缠光子；2013 年，KURODA T 等人利用液滴外延生长砷化镓(gallium arsenide，GaAs)表面的高对称 GaAs/AlGaAs 量子点产生了纠缠光子；2017 年，HUO Y H 等人提出了一种基于砷化钾量子点产生偏振纠缠光量子的方法；2021 年，沈家欣等人提出了一种高对称 GaAs 量子点量子光源的制备方法。2022 年，清华大学甘霖等人基于氮化硼半导体研制出了一种大规模可控制作的高纯度单光子源[19]。2023 年，中科大与新加坡国立大学采用非线性方式，基于 $NbOCl_2$ 材料，研制出了一种厚度仅为 46 nm、可用于光子芯片集成的量子光源[20]。2023 年 10 月日本东京大学的 TAKEZAWA M 等人研究出了一种室温非晶体硅光纤单原子光源，有望解决单光子光源价格昂贵的问题[21]。当前，比较主流的做法是通过激光照射非线性晶体将一个高能光子转换为两个低能的纠缠光子，同时实验人员还能预先知道两个光子的路径，因此可通过测量其中一个光子而判断另外一个路径上是否有单光子。

3.2 量子随机数发生器技术

量子随机数发生器是基于量子叠加态等量子力学特性，随机生成数字序列。量子随机数发生器是人类已知的唯一一种真随机数发生器。1949 年，FRIEDMAN H 提出了人类历史上第一个量子随机数发生方案—基于放射性衰变的随机数发生方案[22]。这种方案有一个明显的缺陷，放射源的强度随时间越来越弱；1994 年，RARITY J G 等人基于单光子探测的方式[23]，根据测量结果产生了原始随机数字；2015 年，中科大研制出了产生速率达 68 Gbps 的量子随机数发生器；2017 年，中国电科网络信息安全有限公司研制出了最高产生速率达 117 Gbps 的量子随机数发生器；2017 年 RAMON 等人充分利用电子载体的电子学优势，提出了一种基于共振隧道二极管提取量子随机信号的方法；2018 年，美国国家标准技术研究院提出了一种设备无关量子随机数发生方法[24]，解决了硬件设备给随机数发生系统带来的安全隐患问题；同年，中科大研制出了具有抗未知器件的可信量子随机数发生器。目前，量子随机数发生器的研究已趋于成熟。

3.3 量子纠缠编码技术

量子纠缠编码，主要用于抵抗量子信道噪声干扰，提高数据传输的可靠性。量子通信的优越性来自于量子的相干性。但是量子的相干性受环境的影响，会随着时间进行指数级衰减，而产生退相干。量子纠错编码就是要解决退相干产生的错误。其中以 CSS 码理论最为成熟。1995 年，SHOR P 基于复杂问题简单化的思想，设计了世界上第一个量子纠错编码方法，将由量子纠缠退相干引起的复杂错误分解为比特翻转、相位翻转和混合翻转等三种简单错误[25]；1996 年，CALDERBANK A R 等人基于经典线性纠错编码原理，提出了一种简单可行的量子纠错编码方案—CSS 码[26]，奠定了量子纠错编码的基础。近年来，研究人员先后提出了量子重复码、量子奇偶校验码等量子纠错编码方法。为了提升量子纠错编码效率，研究人员开展了各种尝试。终于在 2023 年，南方科大的 NI Z C 等人成功将量子相干时间从 694 μm 提高到了 805 μm，超过盈亏平衡点 16%，充分发挥了量子纠错编码的优势[27]。

3.4 单光子探测技术

单光子探测技术主要是利用光电效应原理，通过测量电子状态来探测光子，能够对单光子量级的信号进行响应。单光子探测器主要用于对携带量子信息的单光子进行探测，并转换成电信号进行输出，是接收端的重要组成部分。主要分为基于光电倍增管的单光子探测、基于硅雪崩二极管的单光子探测、基于铟钾砷雪崩二极管的探测和基于超导的单光子探测。其中，基于超导的单光子探测，在红外波段性能优点明显，是单光子探测技术未来的发展方向，也是各国争相发展的重点方向。2023 年，中科院与赋同量子科技共同研制的超导单光子探测器，在 4.2 K 温度时，探测效率达到 70%@15 950 nm，已能够满足基本科学实验使用。但对环境要求苛刻，常温环境下的单光子探测还有待进一步研究[28]。

目前，关于量子光源产生、量子随机数发生、量子

纠缠编码和单光子探测等方面的研究，已经取得了一定成绩，但是还突出存在纠缠光子对产生速率低、纠错编码效率低和光子探测环境要求苛刻等实际问题，距离量子通信工程技术成熟落地尚有一定距离。

4　量子通信应用研究

量子通信应用研究主要基于已有的量子通信协议和量子通信工程技术研究成果，研究和构建实用化量子通信系统，是量子通信研究的落脚点。量子通信应用研究主要包括量子通信链路构建研究、量子通信网络构建研究和量子通信系统构建研究三方面。量子通信链路构建研究主要是搭建量子通信实验环境，构建量子通信链路，解决点对点量子通信问题；量子通信网络构建研究主要是研究量子通信网络架构，以及基于量子通信链路，研究构建量子通信网络，解决多用户点对多点之间的量子通信问题；量子通信系统构建研究面向应用，基于量子通信网络，构建实用化的量子通信系统，解决量子通信的实际应用问题。

4.1　量子通信链路构建技术

量子通信链路构建研究主要是基于量子密钥分发、量子秘密共享、量子隐形传态和量子安全直接通信等协议，进行通信链路构建研究。1982 年，法国物理学家 ALAIN 等人设计试验，验证了微观粒子的量子纠缠现象；1997 年，美国的 TOWNSED [29] 搭建实验环境，首次验证了量子密钥分发技术可行性；同年，奥地利的安东等人首次完成了量子隐形传态原理性验证实验。上述研究为量子通信链路构建的研究奠定了实践基础。

近年来，量子通信链路构建相关研究进展迅速。目前，人类构建的量子通信链路长度可达百公里量级。2006 年，潘建伟团队在世界上首次基于诱骗态量子密钥分发方法，实现了 100 km 的量子密钥分发，标志着量子通信从实验室开始走向工程实用化；2015 年，日本 NTT 公司完成了 100 km 光纤超低损耗量子隐形传态验证实验；2017 年，潘建伟团队利用“墨子号”卫星，完成了世界首次星地量子隐形传态实验，通信距离可达 500 km，为全球化量子通信网络发展奠定了基础；2022 年，龙桂鲁团队基于相位和时间戳量子态混合编码方式，开展了世界最长的量子安全直接通信实验，距离达 100 km。

由于量子信道对光子的衰减是指数级，导致通信距离非常受限，因此要研究量子通信中继技术，延长通信距离。当前，量子通信中继主要有三种类型：一是基于无源光器件的量子密钥分发，可以实现多用户间的时分复用，但是距离有限，不超过 100 km，不具备可扩展性；二是基于可信中继的量子密钥分发，距离远，但是中继必须可信，实际应用受限；三是基于量子纠缠的量子中继，通过在量子通信链路中间设置若干量子中继器进行纠缠交换，可将衰减从指数级降低为多项式级，从而延长量子通信距离 [30]。第三种方式有效解决了通信距离问题，并且实用性较强。当前关于量子通信链路中继的研究主要以第三种方式为基础展开。目前，中国科学技术大学郭光灿团队已经构建了世界最长 833 km 的量子密钥分发链路。

4.2　量子通信网络构建技术

点对点的量子通信链路构建研究只能解决两个节点之间的安全保密通信问题。要进行多用户之间的密钥交换和信息的安全保密传输，就要研究量子通信网络架构，设计量子通信路由协议，构建量子通信网络。

要进行量子通信网络的构建，首先是进行量子通信网络模型的研究。2014 年，王建民构建了一个包括经典通信和量子通信两部分在内的量子通信网络架构模型。其中，量子通信部分主要用于传递量子信息，经典通信部分主要用于辅助量子部分传递经典信息。量子通信部分进一步划分为传输层、控制层和应用层，传输层负责量子通信协议实现，控制层负责通信双方呼叫和连接管理，应用层根据通信方式调用控制层和传输层进行通信和网络管理 [31]，初步解决了量子通信网络架构模型设计问题。2016 年，曹原等人在此基础上，提出了一种基于量子密钥分发的可信光网络体系架构 [32]，主要由应用层、网络层、光网络层和量子密钥分发层以及中央控制器组成。网络层通过路由器，进行灵活的小粒度业务流适配。光网络层通过光交叉连接设备（optical cross connect，OXC），进行高速率、大容量传输。量子密钥分发层通过可信中继节点，进行量子密钥生产和管理，为上层提供安全保密通信。中央控制器负责统一调度，初步解决了基于可信光网络的量子密钥分发网络架构问题。

另外，针对大规模量子通信网络构建问题，2018 年，王健全等 [30] 提出了一种量子密钥分发网络架构，该网络架构根据骨干网和接入网两部分网络，区分为用户节点、接入节点和中继节点三类节点，节点间通过量子信号传输接口、密钥协商接口和密钥中继接口等三类接口进行互联，重点研究解决了量子密钥分发网络大规模分层构建问题。

针对量子通信网络路由协议设计问题，2015 年，荆晶提出了一种自组织的无线量子通信网络模型和一种基于量子纠缠对数目的 AODV 量子通信网络路由协议[33]，基于纠缠量子对数寻找路由，基于两端逼近的纠缠交换方法搭建路由，重点研究解决了量子通信网络路由协议设计和无线量子通信网络构建问题；2017 年，袁小虎，李春文在此基础上，针对非均匀链路光量子通信网络路由协议评价指标，提出应重点考虑路由跳数、最大纠缠度、纠缠资源、路由建立时间、路由可靠性、信道生存时间等因素[34]，研究解决了量子通信网络路由协议设计评价问题。

4.3 量子通信系统构建技术

自 20 世纪 90 年代开始，世界各国普遍加大了对量子通信网络建设的投入力度，并且取得了显著成就，特别是在光纤量子通信系统和卫星量子通信系统建设方面进展迅速，极大地推动了实用化的量子通信系统的发展。典型量子通信系统建设情况见表 2 所列。

表 2 典型量子通信系统建设情况

Tab. 2 Construction of typical quantum communication systems

时间	国家	量子通信系统	建设情况
1997 年	美国	量子密钥分发系统雏形	建成了具有 1 个管理员 +3 个用户的量子密钥分发系统雏形
2002 年	美国	BBN 量子密钥分发系统	BBN 公司基于网络控制器，构建了世界上第一个能够实际应用的量子密钥分发系统
2008 年	奥地利	维也纳量子通信系统	维也纳现场演示了一个 6 节点的量子通信系统，覆盖西门子公司总部和子公司的网络连接，可提供安全保密的电话和视频会议等功能
2010 年	日本	东京量子密钥分发系统	建设了东京量子通信系统，全长 90 km，该网融合了 6 套量子密钥分发系统，距离 50 km 时密钥率可达 100 Kbps，距离 90 km 时密钥率可达 2 Kbps
2014 年	美国	美国量子通信干线	美国航空航天局在局机关和下属的喷气推进实验室之间着手建立一个全长 1 000 km 光纤量子通信干线，并实现与量子通信卫星进行互联，拉开了量子通信的航天应用的大门
2015 年	英国	英国量子通信系统	投资 4 亿英镑建设国家量子通信系统，于 2021 年完成测试
2016 年	俄罗斯	俄罗斯量子通信系统	建成了一个 4 节点的量子通信系统，相邻节点之间距离 30 km ~ 40 km，跻身于世界第一梯队
2016 年	韩国	环首尔量子通信系统	开始建设国家量子通信系统，一期为环首尔地区量子通信系统，于当年完成，全长 256 km。截止 2022 年底，已建成了国家级量子保密通信系统，全长 800 km
2016 年	中国	墨子号量子通信卫星	发射世界首颗量子通信卫星，构建天地一体化量子通信网络雏形，实现了 1 200 km 级地表量子态传输
2017 年	中国	京沪干线	建成世界首条量子保密通信主干网 - “京沪干线”[35]，涵盖北京、合肥、济南和上海等地，全长 2 000 km，可以在相邻的中继站之间进行量子密钥分发，速率大于 20 Kbps，可以满足上万名用户的使用需求，并且“京沪干线”与“墨子号”在北京实现了对接，成功组建了世界上第一个天地一体化量子通信网络，并进行了世界上首次洲际量子通信
2017 年	中国	阿里云量子通信系统	阿里巴巴依托网商银行部署了云上量子加密通信业务，成为全球首个云上量子加密通信案例
2018 年	欧盟	欧盟量子通信卫星	发射了一颗地球低轨道量子通信卫星
2020 年	日本	日本量子通信系统	大力推动量子中继技术研究，为其建设全球量子通信系统打基础
2022 年	德国	耶拿 - 爱尔福特量子通信系统	出资 1 100 万欧元，建设耶拿和爱尔福特之间的量子通信系统[35]
2022 年	中国	量子密钥分发系统	郭光灿团队构建了世界最长的量子密钥分发系统，全长 833 km
2022 年	中国	济南一号	发射世界首颗微纳量子通信卫星，尝试构建低成本、小型化的量子卫星通信系统
2023 年	美国	可操作量子增强通信系统	投资 3 800 万美元，用于建设全球首个可操作量子增强通信系统，提升通信安全性。
2023 年	中国 - 俄罗斯	金砖国家量子通信系统	中俄两国基于墨子号卫星建立了量子通信链路，为金砖国家量子通信系统的建立储备了技术和经验，并进行了有益尝试

关于量子通信链路构建、网络构建和系统构建等方面的应用研究，多由世界科技先进国家组织实施。目前，已经开展了基于卫星、光纤信道的相关量子通信链路构建，在试点城域范围内初步搭建了量子通信网络，并在部分政、商领域进行了试用。后续随着量子通信工程技术的日趋成熟，将逐步拓宽应用范围。

5　结论

通过对量子通信技术及应用研究现状进行分析可知，量子通信自 20 世纪 80 年代诞生以来，发展迅猛。量子通信理论研究相对比较成熟，能够为量子通信技术的应用研究奠定了理论基础; 量子通信工程技术研究进展迅猛，当前已经取得了一定成绩，但是距离技术成熟落地尚有一定距离; 量子通信应用研究，目前正处于蓬勃发展阶段，世界各国为抢得量子通信先机，普遍加大了对量子通信应用的研发和建设投入力度，争抢占领量子通信制高点，取得先发优势。

同时，我们也应该清醒地认识到，量子通信技术及应用研究还存在一些问题亟待解决，突出表现在:

1) 量子通信速率较低。由于量子态产生、传输和检测速率低，导致量子通信速率一直无法得到有效提升。尽管在 10 km 长的光纤信道中，量子密钥分发速率最高可以达到 115. 8 Mbps，但是随着距离的增加，传输速率呈直线下降，距离 325 km 时，仅能达到 200 bps，无法完全满足量子通信系统大规模应用对高带宽的使用需求。未来，有望通过优化量子通信网络架构和采用多路复用技术等方法，不断提高量子通信速率。

2) 量子通信距离较近。由于量子态随距离增加衰减急速增加，严重制约量子通信距离的增加。目前星地传输最远可达 500 km，光纤传输最远可达 833 km，水下通信仅有 10 m 左右，与实际应用对传输距离的要求还有一定差距。随着量子通信中继、量子存储等技术的发展，量子通信距离必将得到大幅提升。

3) 量子通信设备制造和维护成本高。由于光量子的产生需要在超低温环境中进行，量子通信需要高纯度的量子态等因素的限制，导致量子通信设备对材料、工艺、集成和封装等技术要求高，设备价格稳居高位，实验研究和系统建设投入极大。目前量子通信相关研究和建设项目多属国家级行为，要实现普通的商业应用和大众用户使用还有待技术的进步以及行业的标准化等，逐步降低费用，实现大众化应用。

4) 量子通信工程实际安全性受限。尽管量子通信协议基于量子纠缠和海森堡不确定性等量子力学基本原理，在物理理论上是绝对安全的。但是实际工程中量子通信的安全性严重受限于工程技术的发展，量子通信设备和量子传输信道实际上的非绝对安全性严重影响了量子通信理论上的绝对安全性。迫切需要通过改进量子通信设备、技术、协议和算法，开展量子通信系统标准化和安全认证等工作，提高系统安全性。

以上这些问题在一定程度上制约着全球化量子通信系统的进一步发展，同时也为量子通信技术的发展指明了研究方向。未来，随着量子态产生、传输和检测技术的进步，工艺、集成和封装技术的发展，量子通信设备价格的回落，工程实际安全问题的解决，量子通信必将朝着大带宽、远距离、低成本和高安全的方向快速发展。

参考文献:

[1] LIU Y，ZHANG W J，JIANG C，et al. Experimental twin-field quantum key distribution over 1000 km fiber distance [J]. Physical Review Letters，2023，130 (21) : 210801.

[2] DENG Y H，GU Y C，LIU H L，et al. Gaussian boson sampling with pseudo-photon-number-resolving detectors and quantum computational advantage [J]. Physical Review Letters，2023，131(15) : 150601.

[3] WIESNER S. Conjugate coding [J]. ACM SIGACT News，1983，15(1) : 78-88.

[4] BENNET C H，BRASSARD G. Quantum cryptography: public-key distribution and coin tossing [C] //In Proceedings of IEEE International Conference on Computers，Systems and Signal Processing. New York: IEEE，1984: 175-179.

[5] BENNETT C H，BRASSARD G，MERMIN N D. Quantum cryptography without Bell's theorem [J]. Physical Review Letters，1992，68(5) : 557-559.

[6] EKERT AK. Quantum cryptography based on Bell's theorem [J]. Physical Review Letters，1991，67(6) : 661-663.

[7] KULIK S P，MOLOTKOV S N. Measurement-device-independent quantum key distribution [J]. JETP Letters，2023，118(1) : 74-82.

[8] BENNETT C H，BRASSARD G，POPESCU S，et al. Purifi-

cation of noisy entanglement and faithful teleportation via noisy channels [J]. Physical Review Letters, 1996, 76(5): 722-725.

[9] JUNG E, HWANG M R, JU Y H, et al. Greenberger-Horne-Zeilinger versus W states: Quantum teleportation through noisy channels [J]. Physical Review A, 2008, 78(1): 012312.

[10] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613.

[11] GAO G. Multiparty Quantum Secret Sharing Using Two-Photon Three-Dimensional Bell States [J]. Communications in Theoretical Physics, 2009, 52(9): 421-424.

[12] LI H C M. Enhancement of GAO's multiparty quantum secret sharing [J]. Communications in Theoretical Physics, 2011, 56(1): 79-82.

[13] LONG G L, LIU X S. Theoretically efficient high-capacity quantum-key-distribution scheme [J]. Physical Review A, 2002, 65(3): 032302.

[14] 邢莉娟, 李卓, 白宝明, 等. 基于纯态的量子通信系统模型 [J]. 计算机科学, 2008, 35(9): 97-99.

[15] GU B, ZHANG C Y, CHENG G S, et al. Robust quantum secure direct communication with a quantum one-time pad over a collective-noise channel [J]. Science China Physics, Mechanics and Astronomy, 2011, 54: 942-947.

[16] 美科学家在世界上首次制造出原子激光 [J]. 世界科技研究与发展, 1997, 19(2): 104.

[17] 段兆晨, 李金朋, 何玉明. 单光子源及在量子信息领域的应用 [J]. 低温物理学报, 2018, 40(5): 1-16.

[18] WANG X L, CAI X D, SU Z E, et al. Quantum teleportation of multiple degrees of freedom of a single photon [J]. Nature, 2015, 518(7540): 516-519.

[19] GAN L, ZHANG D, ZHANG R, et al. Large-scale, high-yield laser fabrication of bright and pure single-photon emitters at room temperature in hexagonal boron nitride [J]. ACS Nano, 2022, 16(9): 14254-14261.

[20] GUO Q B, QI X Z, ZHANG L S, et al. Ultrathin quantum light source with van der Waals NbOCl2 crystal [J]. Nature, 2023, 613(7942): 53-59.

[21] TAKEZAWA M, SUZUKI R, TAKAHASHI J, et al. Room-temperature addressing of single rare-earth atoms in optical fiber [J]. Physical Review Applied, 2023, 20(4): 044038.

[22] FRIEDMAN H. Geiger counter tubes [J]. Proceedings of the IRE, 1949, 37(7): 791-808.

[23] RARITY J G, OWENS P C M, TAPSTER P R. Quantum random-number generation and key sharing [J]. Journal of Modern Optics, 1994, 41(12): 2435-2444.

[24] BIERHORST P, KNILL E, GLANCY S, et al. Experimentally generated randomness certified by the impossibility of superluminal signals [J]. Nature, 2018, 556(7700): 223-226.

[25] SHOR P. Scheme for reducing decoherence in quantum computer memory [J]. Physical Review A, Atomic, Molecular, and Optical Physics, 1995, 52(4): R2493-R2496.

[26] CALDERBANK A R, SHOR P W. Good quantum error-correcting codes exist [J]. Physical Review A, 1996, 54(2): 1098-1105.

[27] NI Z C, LI S, DENG X W, et al. Beating the break-even point with a discrete-variable-encoded logical qubit [J]. Nature, 2023, 616: 56-60.

[28] ZHANG X F, MA R Y, GUO Z M, et al. Mobile superconducting strip photon detection system with efficiency over 70% at a 1550 nm wavelength [J]. Optics Express, 2023, 31(19): 30650-30657.

[29] TOWNSEND P D. Quantum cryptography on multiuser optical fibre networks [J]. Nature, 1997, 385(6611): 47-49.

[30] 王健全, 马彰超, 李新中, 等. 量子保密通信网络架构及移动化应用方案 [J]. 电信科学, 2018, 34(9): 10-19.

[31] 王建民. 量子通信网络架构及分布式仿真研究 [D]. 西安: 西安电子科技大学, 2014: 61-67.

[32] 曹原, 赵永利, 郁小松, 等. 基于量子密钥分发的可信光网络体系架构 [J]. 信息通信技术, 2016, 10(6): 48-54.

[33] 荆晶. 基于无线自组织量子通信网络的路由算法研究 [D]. 杭州: 浙江工业大学, 2015: 72-75.

[34] 袁小虎, 李春文. 光纤量子通信网络路由选择协议 [J]. 控制理论与应用, 2017, 34(11): 1522-1527.

[35] 康双勇. 量子通信技术发展现状及研究进展 [J]. 保密科学技术, 2017(3): 7-10.

作者简介: 李冲霄(1986—),河北石家庄人,博士研究生,高级工程师。主要研究方向为军事通信。E-mail: lichongxiao126@126.com

通讯作者: 李卓(1980—),陕西西安人,博士,教授,博士生导师。主要研究领域为量子计算、量子信息论、5G 中的编码调制技术。E-mail: lizhuo@xidian.edu.cn